UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/593,302	11/28/2007	Andrew Chow	Q97187	7517

23373 7590 07/30/2009

SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER	
SQUIRES, BRETT S	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
07/30/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/593,302	CHOW ET AL.	
	Examiner	Art Unit	
	BRETT SQUIRES	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 April 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 8 and 9 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Newly added claims 8 and 9 recite "wherein encryption on the fly is performed in real-time," and "wherein decryption on the fly is performed in real-time." The specification does not disclose performing encryption and decryption in real-time and instead the specification discloses performing encryption and decryption on the fly. The examiner now points out that claims 8 and 9 directly depend from independent claim 1, which recites "said encryptor is operable to encrypt on the fly data," and "decrypt on the fly data." Accordingly, the term "real-time," must have a different meaning than "on the fly," in order to differentiate dependent claims 8 and 9 from independent claim 1, and therefore new matter is introduced by the term "real-time."

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-10 are rejected under 35 U.S.C. 103(a) as being obvious over Hearn et al. (US 2005/0091522) in view of Jackson (EP 0911738 A2).

Regarding Claims 1, 6, and 8-9:

Hearn discloses a security device for protecting data (See figs. 1 and 2 ref. no. 35) having an interface ("ATA Cable" and "Bus Control and Interface Logic" See fig. 2 ref. nos. 33 and 43) for connection to a computing device ("CPU" See figs. 1 and 2 ref. no. 13), the security device is located in-line between the interface and the data storage ("Security Device" See figs. 1 and 2 ref. no. 35), a data storage ("Storage Device" See figs. 1 and 2 ref. no. 21), a control system ("Application Program" See paragraph 108), and a memory that includes program data executable on the computing device to perform user authentication ("Flash ROM" See fig. 2 ref. no. 41 and paragraphs 106-108), wherein the control system is configured to expose the memory to the interface to facilitate user authentication and at least until user authentication and to expose the data storage to the interface only upon successful user authentication ("The application program stored in flash ROM 41 for the security device 35 is generally designed to intercept and control the computer system's boot process and provide authentication by means of a login ID and password before access to the protected storage media is permitted." See paragraph 108).

Hearn does not disclose the security device includes an encryptor that is operable to encrypt on the fly data received from the interface and to forward the data

once encrypted to the data storage and decrypt on the fly data received from the data storage and to forward the data one decrypted to the interface.

Jackson discloses a hard disk drive having a dedicated encryption device (See fig. 2 ref. no. 4) connected to the read/write means for encrypting data to be written onto the hard disk drive and decrypting data to be read from the hard disk drive (See paragraph 8).

It would have been obvious to one of ordinary skill in the art at the time of the invention to the security device disclosed by Heard to include a dedicated encryption device such as that taught by Jackson in order to remove the onus from the user to ensure that all files that should be protected by means of encryption are so protected (See Jackson paragraph 7).

Regarding Claim 2:

The above stated combination of Hearn and Jackson discloses the control system is configured to reboot the computing device after successful user authentication and before exposing the encryptor to the interface ("The operating system of the security device 37 then signals the authentication application program run by the host CPU 13 at 120 that the security device bus control and interface logic is configured to adopt the data access profile of the user, whereupon the application program at 121 issues the software interrupt vector to the host CPU13 invoking a warm boot. The appropriate soft boot vector is then loaded and the host CPU 13 causes a soft system re-start or warm boot at step 85." See Hearn paragraphs 143-145).

Regarding Claim 3:

The above stated combination of Hearn and Jackson discloses the memory has a portion of a memory storage system provided with one or more bootable programs ("The security device provides for a custom boot sector to be loaded into the RAM of the host CPU 13, which then executes an authentication application program requiring correct user authentication before allowing the computer system to proceed with its normal boot sector operation and operating system loading." See Hearn paragraph 125).

Regarding Claim 4:

Hearn discloses a security device for protecting data (See figs. 1 and 2 ref. no. 35) having a first interface ("ATA Cable" and "Bus Control and Interface Logic" See fig. 2 ref. nos. 33 and 43) for connection to a computing device ("CPU" See figs. 1 and 2 ref. no. 13), a second interface ("ATA Cable" and "Bus Control and Interface Logic" See fig. 2 ref. nos. 33 and 43) for connection to a data storage ("Storage Device" See figs. 1 and 2 ref. no. 21), the security device is located in-line between the interface and the data storage ("Security Device" See figs. 1 and 2 ref. no. 35), a control system ("Application Program" See paragraph 108), and a memory that includes program data executable on the computing device to perform user authentication ("Flash ROM" See fig. 2 ref. no. 41 and paragraphs 106-108), wherein the control system is configured to expose the memory to the interface to facilitate user authentication and at least until user authentication and to expose the data storage to the first interface only upon successful user authentication ("The application program stored in flash ROM 41 for the security device 35 is generally designed to intercept and control the computer system's boot

process and provide authentication by means of a login ID and password before access to the protected storage media is permitted." See paragraph 108).

Hearn does not disclose the security device includes an encryptor that is operable to encrypt on the fly data received from the first interface and to forward the data once encrypted to the second interface and decrypt on the fly data received from the second interface and to forward the data one decrypted to the first interface.

Jackson discloses a hard disk drive having a dedicated encryption device (See fig. 2 ref. no. 4) connected to the read/write means for encrypting data to be written onto the hard disk drive and decrypting data to be read from the hard disk drive (See paragraph 8).

It would have been obvious to one of ordinary skill in the art at the time of the invention to the security device disclosed by Heard to include a dedicated encryption device such as that taught by Jackson in order to remove the onus from the user to ensure that all files that should be protected by means of encryption are so protected (See Jackson paragraph 7).

Regarding Claim 5:

The above stated combination of Hearn and Jackson discloses the control system is configured to reboot the computing device after successful user authentication and before exposing the encryptor to the interface ("The operating system of the security device 37 then signals the authentication application program run by the host CPU 13 at 120 that the security device bus control and interface logic is configured to adopt the data access profile of the user, whereupon the application

program at 121 issues the software interrupt vector to the host CPU13 invoking a warm boot. The appropriate soft boot vector is then loaded and the host CPU 13 causes a soft system re-start or warm boot at step 85." See Hearn paragraphs 143-145).

Regarding Claim 7:

The above stated combination of Hearn and Jackson discloses the memory includes a bootable program configured to automatically load into the computing device when the device is connected to the computing device and the computing device is powered up ("The security device provides for a custom boot sector to be loaded into the RAM of the host CPU 13, which then executes an authentication application program requiring correct user authentication before allowing the computer system to proceed with its normal boot sector operation and operating system loading." See Hearn paragraph 125).

Regarding Claim 10:

The above stated combination of Hearn and Jackson discloses the security device is physically interposed inline with the ATA cable 33 between the ATA adapter provided on the device interface logic and the storage devices (See Hearn fig. 1 ref. no. 35 and paragraph 100). The above stated combination of Hearn and Jackson further discloses the security device 35 would similarly be interposed between the SCSI drive device and the interface logic (See Hearn paragraph 103).

The above stated combination of Hearn and Jackson does not explicitly disclose the security device is integrated with the computing device through the first interface. However, the examiner respectfully points out that making the security device integral

with the computing device is a matter of obvious engineering choice. See *In re Larson, 340 F.2d 965, 968, 144 USPQ 347, 349 (CCPA 1965).*

Response to Arguments

5. Applicant's arguments filed April 10, 2009 have been fully considered but they are not persuasive.

In response to applicants' argument that the CPU 13 is not involved with the authentication process and therefore Hearn fails to disclose or suggest "a memory that includes program data executable on said computing device to perform user authentication." The examiner disagrees with the applicants' argument and points out that Hearn discloses "the security device provides for a custom boot sector to be loaded into the RAM of the host CPU 13, which then executes an authentication application program requiring correct user authentication before allowing the computer system to proceed with its normal boot sector operation and operating system loading." See paragraph 125.

In response to applicants' argument that if the CPU 37 is considered to be the claimed "computing device," it would not meet the claim requirement for "a memory that includes program data executable on said computing device to perform user authentication," as recited in claim 1. The examiner respectfully points out that the CPU 37 is not being construed as corresponding to the claimed "computing device," but instead CPU 13 is construed as corresponding to the claimed "computing device."

In response to applicants' argument that the dedicated encryption device disclosed by Jackson must receive and authenticate a Crypto Variable or a Crypto Variable and an Initialization Vector before accessing data to encrypt or decrypt and thus does not perform encryption and decryption on the fly. The examiner acknowledges that to enable the dedicated encryption device a Crypto Variable or a Crypto Variable and an Initialization Vector must be input to the dedicated encryption device. However, the examiner points out that the Crypto Variable or the Crypto Variable and the Initialization Vector are input once to enable the dedicated encryption device. After the dedicated encryption device has been enabled "any data read from the drive is automatically decrypted," and "all data written to the drive is automatically encrypted," without re-enabling the dedicated encryption device. See paragraphs 27-28 and 37-38. Accordingly, the dedicated encryption device is operable to encrypt data or decrypt data on the fly once the dedicated encryption device has been enabled.

In response to applicants' argument that the combination of Hearn and Jackson fails to disclose or suggest "wherein said control system is configured to reboot said computing device after successful user authentication and before exposing said encryptor to said interface." The examiner disagrees with the applicants' argument and points out that during the first drive ID stage (See Hearn fig. 4A ref. no. 69) the security device CPU 37 continues to block access to the storage media 21 (See Hearn paragraph 132). The examiner additionally points out that a "warm boot," invokes a special subroutine of the BIOS program that performs an abbreviated start up sequence the proceeds with operation at second startup display screen stage 65 (See Hearn fig.

4B ref. no. 65 and paragraph 145). The examiner now points out that at the second drive ID stage (See Hearn fig. 4B ref. no. 69) the equipment check involving the "drive ID," with respect to the HDD, the operating system of the security device 35 no longer intercepts the request from the host CPU 13 to the protected storage media 21, as long as the access to the HDD of the storage media is in conformance with the particular user data access profile that has been set by the operation of the security device 35 during the first phase of its operation (See paragraph 146).

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRETT SQUIRES whose telephone number is (571) 272-8021. The examiner can normally be reached on 9:30am - 6:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BS/

/Christopher A. Revak/
Primary Examiner, Art Unit 2431